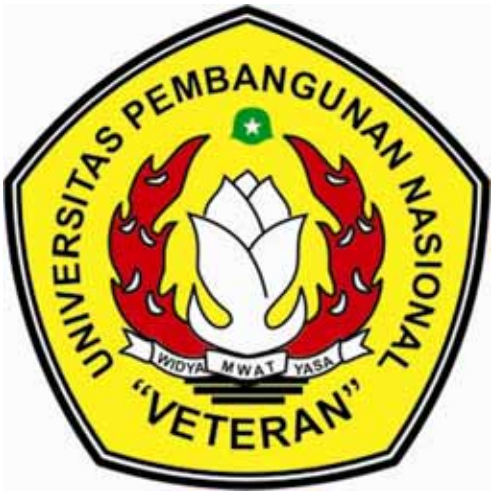
ANALISA DAN DESAIN SECURITY LAYER 2 DENGAN MENGGUNAKAN DHCP SNOOPING PADA JARINGAN HOTSPOT UPN "VETERAN" JAWA TIMUR

SKRIPSI



Diajukan Oleh :
CATUR HIMAWAN SUBAGIO
NPM : 0434010274

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAWA TIMUR
2011

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan kehadirat Allah SWT, atas rahmat, taufik dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi ini, walaupun menyita banyak waktu, tenaga, dan pikiran, namun penulis tetap diberi kesehatan dan semangat kerja yang tinggi. Amin.

Dalam menyusun skripsi ini penulis banyak menerima bantuan, bimbingan dan dukungan dari berbagai pihak. Pada kesempatan ini dengan segala kerendahan hati penulis menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Bapak Ir. Sutiyono, MT selaku Dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional “Veteran” Jawa Timur.
2. Bapak Basuki Rahmat, S.Si, MT selaku Ketua Jurusan Teknik Informatika-FTI UPN “Veteran” Jawa Timur
3. Bapak Prof. Dr. Ir. H. Akhmad Fauzi, MMT dan Bapak Abdullah Fadil, S.Kom selaku dosen pembimbing yang telah membimbing dalam menyelesaikan skripsi ini. Terima kasih atas semua bimbingannya selama menyelesaikan skripsi ini. Terima kasih juga atas semua sarannya yang telah diberikan selama bimbingan.
4. Dosen – Dosen dan staf di Fakultas Teknologi Industri dan Jurusan Teknik Informatika UPN “VETERAN” JATIM, yang telah membantu selama pelaksanaan skripsi ini.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

5. Kedua orang tua tercinta atas semua doa, dukungan serta harapan-harapannya pada saat menyelesaikan skripsi dan laporan ini.
6. Teman-teman kuliah cahyo, teguh, aan, taufan, afif, mahdi, kawan2 kost yang selalu memberikan dukungan, kawan2 soc sby yang selalu memberikan hiburan dan semangat serta semua teman-teman yang mungkin belum saya sebutkan, terima kasih atas segala bantuan, do'a dan dorongan moralnya.

Penulis menyadari bahwasannya dalam penyusunan skripsi ini masih memiliki banyak kekurangan baik dalam segi materi maupun dari segi penyusunannya, mengingat terbatasnya pengetahuan dan kemampuan penulis. Untuk itu, dengan kerendahan hati penulis memohon maaf dan penulis sangat mengharapkan segala saran dan kritikan agar dalam penyusunan selanjutnya lebih baik.

Surabaya, Juni 15 2011

Penulis

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

DAFTAR ISI

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

DAFTAR GAMBAR

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

ANALISA DAN DESAIN SECURITY LAYER 2 DENGAN MENGGUNAKAN DHCP SNOOPING PADA JARINGAN HOTSPOT UPN "VETERAN "JATIM

Penyusun : Catur Himawan Subagio
Pembimbing I : Prof. Dr. Ir. H. Akhmad Fauzi, MMT
Pembimbing II : Abdullah Fadil, S.kom

ABSTRAK

Di dalam kampus Universitas Pembangunan Nasional "Veteran" Jatim terdapat aktivitas jaringan yang begitu kompleks yang pada akhir-akhir ini seringkali mendengar tentang pencurian identitas baik itu pencurian password, akun email atau account lainya. Pencurian identitas ini dilakukan dengan cara *sniffing* atau dalam bahasa Indonesia disebut mengendus. *Sniffing* dapat dilakukan dengan menggunakan beberapa aplikasi yang mampu untuk melakukan pemetaan terhadap *ARP* (*Address Resolution Protocol*) yang berada pada *layer* 2 di dalam jaringan. Kejahatan ini dapat dilakukan dimana saja bahkan pada tingkat kalangan kampus.

Pada penelitian Tugas Akhir ini, akan dilakukan pembuatan suatu *gateway* yang mampu dalam menangani aktifitas *ARP* yang ada pada *layer* 2 di dalam jaringan. Tahapan awal yang ditempuh yaitu pengumpulan data atau literatur tentang *ARP poissoning* kemudian dibuatlah sebuah analisa dan perancangan *gateway layer* 2. Pembuatan mesin *gateway* ini berbasis *open source* dengan menggunakan Linksys WRT 54GL sebagai *hardware* mesin *gateway* dan Open WRT Backfire 10 yang digunakan sebagai sistem operasi yang diterapkan pada gateway.

Guna mengatasi serangan yang dilakukan melalui teknik *ARP poissoning* melalui jaringan *wireless hotspot*, maka UPN "Veteran" Jatim memerlukan sebuah mesin *gateway* yang mampu menangani aktivitas segala aktivitas ARP. Perpaduan antara tekonologi Cisco pada Linksys WRT54GL dan Open WRT ini dipilih karena dari perpaduan teknologi tersebut mampu dalam menangani aktivitas ARP. Dalam kata lain dari perpaduan teknologi ini tidak hanya mampu untuk menyediakan layanan, tetapi juga mampu untuk *preventing system* dari serangan yang dilakukan melalui teknik *ARP poisoning*.

Dari penelitian ini didapatkan hasil uji coba bahwa dengan menggunakan teknik AP Isolation, penyerang yang melakukan serangan pada jaringan yang sudah mengaplikasi atau mengaktifkan AP Isolation hanya mampu menemukan ip dan mac dari gateway itu sendiri. Kesimpulannya adalah penyerang tidak berkutik karena client isolation dari AP.

Kata Kunci: *sniffing, snooping, ARP poisoning, jaringan, hotspot.*

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era perkembangan teknologi telekomunikasi dan teknologi komputer saat ini sudah sangat cepat sekali. Berbagai produk alat-alat komunikasi dan komputer serta aplikasi-aplikasi guna mendukung arus informasi sudah banyak diciptakan, contoh kecil dari produk teknologi informasi adalah IP (*Internet Protocol*) *address* yang telah menciptakan komunikasi antara PC (*Personal Computer*) satu dengan PC yang lain. Dengan demikian hampir siapa saja dapat saling bertukar informasi melalui media jaringan baik itu jaringan kabel atau jaringan tanpa kabel (*nirkabel*).

Dalam pendistribusian suatu IP dapat dibedakan menjadi dua macam yakni, distribusi IP secara static dan distribusi IP secara otomatis. Sebagian besar instansi-instansi menggunakan DHCP (*Dynamic Host Configuration Protocol*) *server* sebagai layanan untuk pengalokasian IP secara otomatis agar memudahkan pengalamatan suatu IP *address*.

Penggunaan DHCP dalam pengalokasian IP ke *client* di dalam sebuah jaringan LAN, DHCP snooping dapat diaktifkan guna meningkatkan keamanan jaringan dalam LAN tersebut. Pemanfaatan DHCP snooping pada sebuah jaringan LAN ini memungkinkan *client* untuk mengakses jaringan secara privat, privat dalam artian IP dan MAC address dari *client* akan diisolasi oleh router.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

Selain menggunakan DHCP di dalam jaringan wireless untuk mengamankan jaringan pada umumnya digunakan WEP. WEP (Wired Equivalent Privacy) merupakan suatu algoritma eknripsi yang digunakan oleh shared key pada proses authentikasi untuk memeriksa user dan untuk melakukan enkripsi data yang dilewatkan. Akan tetapi pemanfaatan WEP bersifat shared dimana client yang mengetahui shared secret dari WEP akan terkoneksi dengan mudah dan dapat mengirimkan ARP attack terhadap pengguna jaringan yang lain.

Berkaitan dengan tugas akhir ini penelitian difokuskan pada masalah pemanfaatan teknologi *open source* yang dapat memberikan dukungan terhadap aktifitas kelancaran data di dalam jaringan.

Penelitian ini dilaksanakan pada UPT (Unit Pelaksana Teknis) Telematika UPN “Veteran” Jawa Timur, Surabaya. UPT Telematika merupakan pusat pelayanan data baik itu pelayanan data jaringan internet dan data jaringan lokal antar fakultas. Layanan akses jaringan internet sering kali disalah gunakan oleh pihak-pihak tertentu dengan maksud dan tujuan yang tentunya berbeda-beda, mulai dari memutuskan koneksi antar client, pencurian account dan beberapa aktifitas lain yang merugikan.

1.2 Rumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan di atas, maka rumusan masalah yang akan dikaji di dalam penelitian ini sebagai berikut:

a. Bagaimana melakukan tindakan pencegahan terhadap jaringan komputer mulai dari client hingga gateway agar terhindar dari serangan DHCP *snooping* dengan teknik ARP poisoning.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

b. Bagaimana memanfaatkan teknologi Cisco pada sebuah *access point* agar dapat dijadikan sebagai *super router*.
c. Bagaimana melakukan tidakan *isolasi* antar *client* agar terhindar dari serangan DHCP *snooping* dan ARP poisoning lainnya.

1.3 Batasan Masalah

Agar permasalahan terfokus pada suatu permasalahan di atas, maka ditentukan batasan masalah sebagai berikut di bawah ini:

a. Analisa sistem keamanan jaringan ini menggunakan perangkat Wireless Router WRT54GL sebagai super router.
b. *Router OS* menggunakan OpenWRT Backfire 10.3 Released sebagai sistem operasi pada router.
c. Menggunakan *tools* Netcut, Tuxcut, Ettecap sebagai alat uji simulasi guna meracuni ARP pada jaringan yang ada.
d. Pengujian *system* keamanan ini dilakukan dengan cara melakukan ARP poisoning terhadap *client* melakukan koneksi terhadap *router* atau *gateway* melalui *wifi* atau jaringan nirkabel.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang penulis kaji maka penelitian ini memiliki untuk mendesain dan menganalisa terhadap security pada layer 2 dengan menggunakan DHCP snooping dan dampaknya di UPN “Veteran” Jatim agar terhindar dari ARP poisoning.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

1.5 Manfaat dan Hasil Penelitian

Manfaat yang dapat diambil dari Tugas Akhir ini adalah:

a. Terhindar dari pihak yang tidak bertanggung jawab yang secara sengaja memutuskan hubungan koneksi jaringan yang jaringan wifi.
b. Terhindar dari pencurian data baik itu pencurian password, permodifan content email, dan lain-lain yang dapat dilakukan dengan cara ARP poisoning.
c. Menjaga integritas data antar client yang terkoneksi dengan router / gateway.
d. Kerahasiaan data antara client dengan client dapat terjamin.

1.6 Metode Penulisan

Langkat-langkah pengumpulan data sebagai dasar penyusunan Tugas Akhir ini adalah sebagai berikut:

a. Metode Analisa

   Menganalisa masalah-masalah yang akan disajikan dan mengumpulkan data atau informasi.

b. Metode Literatur

   Merupakan usaha untuk lebih memudahkan dalam melengkapi data dan memecahkan masalah yang merupakan sumber referensi bagi penulis dalam mengambil langkah pengamatan dan melengkapi data.

c. Metode Observasi

   Observasi merupakan aktivitas melakukan pengamatan dan anlisa terhadap kondisi sebenarnya di lapangan dan akan diberikan solusinya.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

d. Metode Implementasi

Merukapan aktivitas melakukan pengerjaan sistem mulai dari desain hingga pembuatan system keamanan jaringan dengan OpenWRT.

e. Evaluasi

Evaluasi dari hasil-hasil yang telah dikerjakan

1.7 Sistematika Penulisan

Dalam laporan Tugas Akhir ini pembahasan disajikan dalam enam bab, berikut sistematika dari penulisan Tugas Akhir ini:

BAB I PENDAHULUAN

Berisi latar belakan yang menjelaskan tentang pentingnya penelitian Tugas Akhir yang dilakukan, rumusan masalah, tujuan, manfaat, metodologi dan sistematika penulisan yang digunakan dalam laporan Tugas Akhir ini.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan tentang teori-teori yang berkaitan dengan isi laporan Tugas Akhir dan sistem keamanan yang dibuat dan komponen-komponen lain yang digunakan dalam pembangunan sistem keamanan ini.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang tata cara metode perancangan sistem security yang digunakan untuk mengolah sumber data yang dibutuhkan sistem.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.

BAB IV IMPLEMENTASI SYSTEM

Pada bab ini menjelaskan tentang implementasi dari system security yang telah dibangun meliputi lingkungan implementasi, skenario uji coba, dan pengujian serangan jaringan dengan metode ARP poisoning.

BAB V UJI COBA DAN EVALUASI

Pada bab ini menjelaskan tentang pelaksanaan uji coba dan evaluasi dari hasil uji coba sistem yang telah dibuat sebelumnya.

BAB VI PENUTUP

Bab ini berisi tentang kesimpulan yang dapat diambil dari keseluruhan isi dari laporan Tugas Akhir serta saran yang disampaikan penulis untuk pengembangn sistem yang ada demi kesempurnaan sistem yang lebih baik.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembuatan laporan Tugas Akhir.

Hak Cipta © milik UPN "Veteran" Jatim :
Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber.